UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/538,517	03/29/2000	Jun Maruo	SONY-50N3505	6696

7590 08/10/2005

Wagner Murabito & Hao LLP
Two North Market Street
Third Floor
San Jose, CA 95113

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/538,517	MARUO ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *34-44* is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1- 44 are pending.

Reopening of Prosecution - New Ground of Rejection After Appeal 1.

2. In view of the Appeal Brief filed on 2/8/2005, PROSECUTION IS HEREBY REOPENED. A new ground of rejection set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111; or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. **Claims 1-6, 9-16, 18-20, and 23-33** are rejected under 35 U.S.C. 102(b) as being anticipated by Davis U.S. Patent No. 5,825,879.

As per claims 1and 13, Davis teaches a transceiver system for receiving content contained in a secure digital broadcast signal, comprising:

a first component for generating a data stream [fig.4, Image generation device 400];

a first encryption unit coupled to the first component, and for encrypting the data stream for transmission to generate an encrypted data stream [Frame Data Encryptor 320];

a second component for generating a video signal for a display device [col. 5, lines 50-55, image display device or IDD 404];

a second encryption unit coupled to the second component and for decrypting the encrypted data stream received from the first component [Frame Data DECRYPTOR 324]; .

a bidirectional digital bus coupled to the first encryption unit and the second encryption unit [fig. 4, authenticated secure path 408, col. 5, lines 47-59, see also fig. 3, element 3, col. 5, line 31-39, a communication path between encryptor and decryptor]; and

a third component [fig. 4, MANAGEMENT PROCESSOR OR STE MACHINE 436 and associated text, see also fig. 2, management processor 240 and the associated text] coupled to the bus for arbitration such that content from the data stream is securely transferred across the bus and without exposing an unencrypted data stream [fig. 2 and associated text, col. 5, lines 5-11, control lines 224 coupling a management processor 240 to the Secure Video Content processor (SVCP) and that the management processor 240 manages and coordinates the operation of the SVCP) such that transmission of digital image frames outside the SVCP is encrypted and secure (col. 5, lines 19-31, see also col. 4, lines 64 through col. 7line 3, where Davis discloses that the management processor determines when a display device will require particular frames of data and that when particular frame is needed, the particular frame is retrieved from the frame buffer and decrypted using the obtained key from the encryption circuitry].

As per claims 2, Davis teaches the system of claim 1 wherein the transceiver is a set-top box [col. 7, lines 14-20].

As per claims 3, 15, and 18, Davis teaches the system/architecture of claims 1 and 13 respectively, wherein the first component is an audio video decode block for decoding the data stream from a digital broadcast signal [col. 4, lines 56-57, decryption and decompression circuitry 228, where decryption and decompression circuitry decrypts and decompresses the data stream, see also col. 5, line 60 through col. 6, line 9].

As per claims 4 and 16, Davis teaches the system/architecture of claims 1 and 13 respectively, wherein the second component is a graphics block for generating the video signal from the data stream received from the first component [col. 5, lines 1-5, see also fig. 4 and associated text disclosing IDD 404 including management processor 436, Digital Analog Converter 448 and Frame data decryptor 444].

As per claims 5 and 19, Davis teaches the system/architecture of claims 1 and 13 respectively, wherein the third component is a CPU (central processing unit) block coupled to the bus for managing an encryption process of the first encryption unit and the second encryption unit (col. 5, lines 9-11 discloses that management processor 240 manages and coordinates the operation of the SVCP which includes encryption processes in IGD in IDD, see also col. 6, lines 64-67].

As per claims 6 and 20, Davis teaches the system/method of claims 5 and 19 respectively, wherein the encryption process is key-based encryption process and the CPU block manages the distribution of keys to the first encryption unit and the second encryption unit [col.6, line 64 through col. 7, line 3].

As per claims 9 and 23, Davis teaches system of claims 1 and 19 wherein said data stream is encrypted using an encryption process compliant with DES (Data Encryption Standard Electronic code book) [col. 6, lines 35-41).

As per claims 10 and 24, Davis teaches the system/ architecture of claims 1 and 19 respectively, wherein the bus is a PCI (Peripheral Component Interconnect) compliant bus and each encryption unit performs encryption and decryption [col. 3, lines 44-46].

As per claim 11, Davis teaches the system of claim 1further comprising a front end block coupled to the bus for receiving the digital broadcast signal and generating the data stream therefrom [col. 3, lines 56-61, where an outside source 120 (front end) provides an encrypted digital data stream along a connecting cable 124 to the PC 100 and interconnecting buses 128 such as PCI buses, transfer data among the various elements], the first component coupled to receive the data stream from the front end block via the bus [the Decryption Circuitry and Decompression Circuitry 228 (fig. 2 and associated text) of the SVCP receives the encrypted data stream from the front end via the bus].

As per claims 12, Davis teaches the system of claim 1, wherein the data stream is substantially compliant with a version of the MPEG (Moving Pictures Experts Group) format [col. 1, lines 38-40], see also col. 4, lines 49-55].

As per claim 14, Davis reaches the architecture of claim 13 wherein the first component and the first encryption unit are built into a first integrated circuit device and the second component and the second encryption unit are built into a second integrated circuit device (col. 5, lines 51-59, i.e. SVCP is partitioned into two parts, IGD (image generation device) and IDD (image display device)).

As per claim 25, Davis teaches in a transceiver for receiving a digital broadcast signal, a method for implementing secure transmission of data from the digital broadcast signal between internal components of the transceiver via a bus, the method comprising the steps of:

a) accessing a digital broadcast signal using a first component of a transceiver (fig. 4 , DECRYPTION CIRTCUITRY AND DECOMPRESSIN CIRCUITRY 416 of the IMAGE GENERATING DEVICE 400);

b) generating a data stream by descrambling the digital broadcast signal using the first component (DECRYPTION CIRTCUITRY AND DECOMPRESSIN CIRCUITRY 416 of the IMAGE GENERATING DEVICE 400);

c) encrypting the data stream using a first encryption unit to generate an encrypted data stream [Frame Data Encryptor 320];

d) transmitting the encrypted data stream to a second component via a bus [fig. 4, authenticated secure path 408, col. 5, lines 47-59, see also fig. 3, element 3, col. 5, line 31-39, a communication path between encryptor and decryptor]; and

e) decrypting the data stream using a second encryption unit coupled to the second component such that the bus carries only an encrypted version of the data stream and without exposing an unencrypted data stream [fig. 4, Frame Data DECRYPTOR 444, see associated text, col. 6, lines 10-23, where the frame data decryptor 444 decrypts the received data without compromising the data (col. 6, lines 7-9).

As per claim 26, Davis teaches wherein the transceiver is a set-top box [col. 7, lines 14-20].

As per claim 27, Davis teaches wherein the bus is a PCI (Peripheral Component Interconnect) compliant bus and each encryption unit performs encryption and decryption [col. 3, lines 44-46].

As per claim 28, Davis teaches wherein the first component is an audio video decode block for decoding the data stream from a digital broadcast signal [col. 4, lines 56-57, decryption and decompression circuitry 228, where decryption and decompression circuitry decrypts and decompresses the data stream, see also col. 5, line 60 through col. 6, line 9].

As per claim 29, Davis teaches wherein the second component is a graphics block for generating the video signal from the data stream received from the first component (col. 5, lines 1-5, see also fig. 4 and associated text disclosing IDD 404 including management processor 436, Digital Analog Converter 448 and Frame data decryptor 444).

As per claim 30, Davis teaches wherein the third component is a CPU (central processing unit) block coupled to the bus for managing an encryption process of the first encryption unit and the second encryption unit (col. 5, lines 9-11 discloses that management processor 240 manages and coordinates the operation of the SVCP which includes encryption processes in IGD in IDD, see also col. 6, lines 64-67].

As per claims 31, Davis teaches wherein the encryption process is key-based encryption process and the CPU block manages the distribution of keys to the first encryption unit and the second encryption unit [col.6, line 64 through col. 7, line 3].

AS per claim 32, Davis teaches wherein said data stream is encrypted using an encryption process compliant with DES (Data Encryption Standard Electronic code book) [col. 6, lines 35-41).

As per claims 33, Davis teaches wherein the data stream is substantially compliant with a version of the MPEG (Moving Pictures Experts Group) format [col. 1, lines 38-40], see also col. 4, lines 49-55].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 7 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis as applied to claim 5 and 19 above, and further in view of Summers et al. (prior art of record).

As per claims 7 and 21, Davis does not teach but Summers et al. (prior art of record) teach the system/architecture of claims 5 and 19 respectively, further comprising an arbiter coupled to the CPU block for arbitration of the bus (see figure 4, SECURE BUS ARBITER 40 of Summers et al.).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the Summers' secure bus arbiter within the system/method of Davis with a motivation to provide a simplified security to Davis's SVCP and to prevent unauthorized elements of the Davis's personal computer to intercept or alter the content (Summers, col. 1, lines 22-27).

5. Claims 8 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis as applied to claims 1 and 19 above, and further in view of Computer Architecture and Organization to John P. Hayes (prior art of record).

As per claims 8 and 22, Davis is silent in disclosing the system/architecture of claims 1 and 19 wherein the first component, second component, and third component include respective identification registers for identifying each co respectively, wherein the first component, second component, and third component include respective identification registers for identifying each component.

However, Hayes does disclose an the system/method of claims 1, 19, and 34 respectively, wherein the first component, second component, and third component include respective identification registers for identifying each component (see page 139, Circuit specification, second paragraph].

Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Hayes' teachings such that each component of Davis's system have a register therein. One of ordinary skill in the art would have been motivated to modify Davis's system as such in order to allow for the management processor to identify the present state of the component.

6. Claim 17 is rejected under 35 U.S.C. l03 (a) as being unpatentable over Davis as applied to claim 13 above, and further in view of U.S. Patent No. 5,872,846 to lchikawa (prior art of record).

As per claim 17, while Davis teaches the decryption circuitry and the decompression circuitry 228 (fig. 2, col. 4, lines 59-60) for decrypting and decompressing the digital broadcast signal, Davis is silent in disclosing the architecture of claim 13 wherein the first component is a conditional access block for descrambling the digital broadcast signal.

However, Ichikawa does disclose the architecture of claim 13 wherein the first component is a conditional access block for descrambling the digital broadcast signal (see figure 3, First-Level Decoder 332, Key 308).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Ichikawa's teachings of a conditional access block such that the first component of Davis. is a conditional access block. One of ordinary skill in the art would have been motivated to modify Davis's system as such in order to allow only the authorized subscriber to obtain.

7. Claims 34-41 are allowed over prior art of record.

Conclusion

7. Prior arts made of record, not relied upon:

US Patent 6,751,321 to Kato et al. is directed to a source of MPEG2 video data is connected with a dedicated AV device or personal computer by means of an IEEE 1394 interface. A transmission unit in the source has an IEEE 1394 encryption unit and a sending I/F unit. A reception unit varies between the dedicated AV unit and the personal computer. In the reception unit of the dedicated AV device, a receiving I/F unit and a decryptor are integrally incorporated into one semiconductor chip and an MPEG2 decoder is incorporated into one semiconductor chip. In the reception unit of the personal computer, the receiving I/F unit is formed of one semiconductor chip, and the decryptor connected to the I/F unit through a bus, and the MPEG2 decoder are formed of one semiconductor chip. Thus, data before decryption will not appear on the bus, which prevents MPEG2 video data from being taken out of the computer for illegal copying purposes. In addition, the reception unit is made to have a different physical

configuration depending on whether it is to be mounted in the dedicated AV device or the personal computer. This will prevent the reception unit (including the decryptor) of the dedicated AV device from being connected in the personal computer in place of its associated reception unit (excluding the decryptor).

US Patent No. 6, 286,103 to Maillard et al. is directed to a method and apparatus for the transmission and reception of scrambled data is disclosed. In some embodiments, the method and apparatus includes transmitting a scrambled data stream to a decoder, sending the scrambled data stream to a portable security module inserted in the decoder, descrambling the scrambled data stream, encrypting a descrambled data stream, and using the encrypted data stream to the decoder, decrypting the encrypted data stream, and using the decrypted data stream.

US Patent No. 5,455,862 to Hoskinsom is directed to an encryption/decryption unit (EDU) and method for determining a data encryption key used in encrypting and decrypting data transmitted over a non-secure communication link. Each EDU includes a central processing unit (CPU) that controls its operation, random access memory (RAM) in which one or more sets of seed keys are stored, and a data encryption standard (DES) coprocessor that implements a data encryption algorithm developed by the U.S. National Bureau of Standards. The CPU includes special circuitry enabling it to operate in an encrypted mode so that it cannot be interrogated to discover the program or data stored therein. Each EDU randomly generates a pointer, bytes of which determine the number of times that a loop is repeated in which values (initially determined by two of the seed keys) are XORed together and encrypted using one of the seed keys to determine a portion of the data encryption key (DEK). The pointer is encrypted, along with other information, producing an encrypted key header that is transmitted to the other EDU establishing

the link. Upon receiving the encrypted key header, it is decrypted, and the decrypted pointer is used by the receiving EDU to determine the portion of the DEK developed by the other EDU. The two portions of the DEK are then logically combined at each EDU to produce the final DEK, which is then used during the current communication session for encrypting data exchange between the two EDUs.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T. Arani

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

8/6/05